Customer No. 24498
Attorney Docket No. PD030108
Office Action Date: 09/29/2008

REMARKS

This application has been reviewed in light of the Office Action dated September 29, 2008. Claims 1-8, 10 and 11 are pending in the application. Through prior amendments, claim 9 has been cancelled without prejudice. By the current amendment, claim 5 has been cancelled without prejudice and its subject matter has been added to claims 1 and 6. Claims 1, 3, 4, 6, 8 and 10 have been amended. In addition, new claim 12 has been added. No new matter is believed to be added.

Independent claims 1 and 6 have been amended to recite "decrypting the second data set using a second of said decryption keys, wherein the second decryption key is not used for decrypting the first data set." Support for this amendment is found in the specification on page 10, lines 21-26 ("The supplement data… is encrypted by a *second encryption key* that is compatible, but *not identical, to the first encryption key*") and page 12, lines 27-30 ("In one embodiment of the invention, the removable storage device may hold more than one decryption key, wherein *at least one key may be used for decryption of supplementary data*"). The quoted paragraph on page 12 continues by referring to the key used to decrypt the supplementary data as "the separate key." Therefore, the specification as filed supports the feature of having more than one key present on the removable storage device and where the encryption of the supplemental data is not identical to the first key such that a second key is needed for decryption.

-6-

PAGE 6/11 * RCVD AT 1/8/2009 3:56:50 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/15 * DNIS:2738300 * CSID:609 734 6888 * DURATION (mm-ss):01-58

Rejections under 35 U.S.C. 102(e)

By the Office Action, claims 1, 3, 5, 6, 8 and 11 stand rejected under 35 U.S.C.

102(e) as being anticipated by U.S. Patent Application Publication 2003/0072453 to Kelly,

et al (hereinafter Kelly). The Examiner's reconsideration of the rejection in view of the

above amendments and the following arguments/remarks is respectfully requested.

Kelly is directed to a method of making available additional content related to

basic content in a secure way. Kelly discloses that the basic content is distributed on a

record carrier and protected by a security mechanism. Kelly teaches a security mechanism

whereby each record carrier has an encrypted disc key which can be decrypted by the

playback device. The playback device then uses the disc key to decrypt the title key or

keys associated with the basic content stored on the record carrier. Kelly further teaches

that the additional content, which is available on a server for download, is protected by the

same mechanism as the basic content, employing at least one of the same keys.

Kelly does not, however, teach or suggest a method wherein "at least two

respective device independent electronic decryption keys are stored on a removable

prerecorded storage medium" comprising the steps of, *inter alia*, "decrypting the first data

set using a first of said decryption keys; and decrypting the second data set using a second

of said decryption keys, *wherein the second decryption key is not used for decrypting the*

first data set," as recited in claim 1 and essentially recited in claim 6.

While Kelly does teach two encryption keys (i.e. an Encrypted Disc Key,

hereinafter EDK, and an Encrypted Title Key, hereinafter ETK), Kelly teaches that both of

these keys **must be used together** to decrypt the basic content, *i.e.* the first data set. Fig. 2

and paragraphs [0034-0035 and 0044] of Kelly describe that each sector of content on the disc is encoded by an ETK. In order to decrypt the content, Kelly teaches that, first, the EDK is decrypted using a key present on the playback device. Then, the ETKs, which are used to decrypt the content, are decrypted using the EDK. Kelly further discloses that the additional content, *i.e.* the second data set, is protected by the same security mechanism as the basic content. As such, the additional content is decrypted using the same keys that decrypt the basic content (see abstract lines 9-10, and paragraphs [0008, 0012, 0014, 0019, 0051, 0058]).

Claims 1 and 6, as amended, clearly recite that the second decryption key is <u>not</u> <u>used for decrypting the first data set</u>. Nothing in Kelly even remotely suggests this feature of claims 1 and 6. In fact, as discussed above, Kelly's second key (the ETK) is required to decrypt the basic content on the record carrier. Thus, Kelly actually teaches away from the above mentioned feature of amended claims 1 and 6.

While Kelly does disclose an alternate embodiment in which the EDK and ETK are not used to decrypt the supplemental content, this embodiment also fails to teach each and every limitation of amended claims 1 and 6. In paragraph [0059], Kelly discloses that instead of the EDK and ETK, a Session Key can be used to decrypt the additional data. While this could be a second key which is not used to decrypt the first data set, the Session Key is not stored on the prerecorded storage medium. Kelly teaches that the Session Key is derived by the server from which the additional content is being retrieved. In contrast, claims 1 and 6 clearly recite that the first and second keys "are stored on a removable

Customer No. 24498
Attorney Docket No. PD030108
Office Action Date: 09/29/2008

prerecorded storage medium." Thus, this embodiment of Kelly also teaches away from amended claims 1 and 6.

For at least the foregoing reasons, claims 1 and 6 are believed to be patentably distinguishable over Kelly. Additionally, claims 3, 5, 8 and 11 are believed to be patentably distinguishable over Kelly at least by virtue of their dependency on claims 1 and 6. Reconsideration of the rejection is respectfully requested.

Rejections under 35 U.S.C. 103(a)

By the Office Action, claims 2 and 7 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Kelly in view of U.S. Patent No. 6,529,949 to Getsin et al (hereinafter Getsin). Also by the Office Action, claim 4 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Kelly in view of U.S. Patent Application Publication 2002/0176575 to Qawami et al (hereinafter Qawami). Further, claim 10 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Kelly in view of NPL: Schneier, Bruce, "Applied Cryptography," 2nd Edition, 1996, pages 1-14 (hereinafter Schneier).

However, claims 2, 4, 7 and 10 are all dependent from claims 1 or 6. Moreover, the 103(a) rejections of claims 2, 4, 7 and 10 cite only Kelly as teaching the elements of claims 1 and 6 which are present in these claims through dependency. Thus, Applicants believe that these claims are patentably distinguishable over any combination of the cited references for at least the reasons discussed above with reference to the 35 U.S.C. 102 rejections. Reconsideration of the rejections is respectfully requested.

-9-

Customer No. 24498
Attorney Docket No. PD030108
Office Action Date: 09/29/2008

In view of the foregoing amendments and remarks, it is respectfully submitted that all the claims now pending in the application are in condition for allowance. Early and favorable reconsideration of the case is respectfully requested.

It is believed that no additional fees or charges are currently due. However, in the event that any additional fees or charges are required at this time in connection with the application, they may be charged to Applicant's representatives Deposit Account No. 07-0832.

Respectfully submitted,

Dated: 1/8/09

By: _____
Paul P. Kiel
Registration No.: 40,677

THOMSON LICENSING LLC
PO BOX 5312
PRINCETON, NJ 08540

-10-